A BDO LEGAL GUIDE TO EUROPEAN TECH REGULATIONS:

A concise overview for companies

BDO

A BDO Legal Guide to European Tech Regulations: A concise overview for companies

Companies in the Tech sector face many new European regulations, and it is important to know which of these rules apply to your company. This overview is intended to give you a quick insight and help guide you through the most important aspects of a selection of these European Tech regulations.

STARTING POINT

To keep this document concise, a selection of the most relevant company types and regulations has been made. Not all types of companies affected by the new regulations are included, and only the most significant of the new European rules are considered.

Which regulations are applicable to you depends on the size of your business, the type of business and the business activities.

The below table provides an insight into activities and businesses that may be covered by the new rules. **Clicking on the applicable regulation in the right-hand column will take you to a summary of the main points of interest.**

Multiple schemes may be relevant to one company.

It should be noted the content of these laws and regulations may change in the future and that we may issue updated versions of this whitepaper. Please contact us for the most up to date information.

ACTIVITY/TYPE OF BUSINESS	IF YES, SEE REGULATIONS
Does your company operate in energy, transport, banking, financial market institutions, health, drinking water, wastewater, digital infrastructure, government services, aerospace, postal and courier services, waste management, chemicals, food, manufacturing, digital providers?	• NIS2
Are you a manufacturer of IoT devices (processing/generating data about their use or environment and sending it over the internet)?	• Data Act
Are you a provider, importer, distributor or user of software or products containing artificial intelligence systems?	• Artificial Intelligence Act
Are you a digital service provider, designated as a "core platform service" c.q. "gatekeeper" (Large online search engine, brokering service, social network, video platform and the like)?	• Digital Markets Act • Digital Services Act • DAC7 • NIS2
Do you operate an online search engine?	• Digital Markets Act • Digital Services Act
Do you operate an (employment) platform that operates at least partly online and is focused on commercial services provided by individuals, which may include (online) delivery services, transport services, cleaning services and staffing services?	• Directive on Platform Work • DAC7 • Digital Services Act
Are you an internet service provider or hosting provider (transmission or temporary or otherwise storage of information of online platform users)?	• Digital Services Act
Do you operate an online platform, not designated as a gatekeeper, that stores and disseminates information provided by its users to the public (social media platforms, online marketplaces and other platforms with User Generated Content)?	• Digital Services Act
Do you operate an online platform focused on real estate or transport rental, provision of personal services, sale of goods?	• DAC7
Do you supply software intended to be used alone or in combination with hardware for one or more specific (human) medical purposes?	• Medical Device Directive
Are you a public body?	• Data Governance Act • Data Act
Are you a data intermediary, data processing service or another type of data receiving/holding/managing organisation?	• Data Governance Act • Data Act
Are you a financial institution or do you provide financial services/products (credit institution, crowdfunding service, account information provider, insurance intermediary, trading platform, data analytics and data centre services, e-money institutions, crypto asset services)?	• NIS2 • DORA

In brief, what do the regulations entail?

Data Governance Act

WHAT IS IT ABOUT?

The Data Governance Act (DGA) is a European regulation created within the framework of the European data strategy and is mainly about data sharing in the public sector, the use of data sharing services and data altruism.

Data has significant potential for economic growth and social progress, such as improved healthcare and innovation. For example, good data management and data sharing are beneficial for developing better policies by government bodies and necessary for training AI systems.

However, barriers such as lack of trust and technical obstacles limit data sharing in the European Union. The DGA aims to address these barriers. With the DGA, the European Union aims to stimulate innovation, promote responsible and transparent data management, increase trust in data sharing and facilitate data reuse for the benefit of European citizens and businesses. **By introducing the DGA, the European Union expects benefits for companies and individuals through the use of large amounts of health data, mobility data, environmental data, agricultural data and public administration data, among others.**

The DGA regulates four main topics:

- First, **the DGA sets conditions for the (wider) reuse of public sector data**, even if it is protected by, for example, commercial confidentiality, intellectual property rights or privacy laws. By introducing the DGA, this public sector data can be more easily reused. It is worth noting that the DGA focuses on non-personal data and that if the data in question does involve personal data, the General Data Protection Regulation (GDPR) still applies.

- Second, **the DGA provides a framework for data sharing services to ensure that they will act as trusted intermediaries of data exchange within the common European data spaces**. The DGA contains rules on the establishment, supervision and practices of these intermediaries. These include neutrality and transparency. For example, these neutral third parties cannot make money from the transfer of data, but their main aim is to make the transfer of data easier. In this way, the DGA offers an opportunity to form a stronger front against the Big Tech platforms, which occupy an important market position due to the large amount of data they possess.

- In addition, **the DGA includes measures to make it easier for citizens and companies to make their data available for the benefit of society**. Data altruism refers to individuals and companies who voluntarily and without any remuneration approve the making available of data they generate themselves, to use this data for the public interest. Data altruism organisations are subject to DGA rules. Among other things, such organisations are expected to register and comply with associated registration requirements, including those that the organisation must be non-profit in nature and meet transparency requirements.

- Finally, **the introduction of the DGA establishes a European Data Innovation Board (EDIB)** to promote the above points.

Data Governance Act

WHAT CAN YOU DO?

The regulation will have relatively little impact on most businesses. **The regulation is particularly relevant for public authorities, data intermediaries and organisations seeking to make certain data freely available.** For them in particular:

- **Ensure that (cooperation) agreements comply with the regulation**, e.g. do not include exclusivity clauses limiting reuse of data by third parties.
- **Ensure that there is a clear separation between activities that see generation/sharing of data and other business activities where data may be monetised.**

In brief, what do the regulations entail?

Data Act

WHAT IS IT ABOUT?

Currently, much IoT data is only available to the manufacturer of the product or their service companies. By introducing the Data Act, the European Union hopes that this data will not go unused but is available to create new innovative services also in other sectors.

The Data Act gives users – both businesses and consumers – **access rights to data generated in connected products owned by them**. This covers a wide range of IoT devices ranging from home appliances to trucks, machinery, or airplanes. Data generated from connected products will be available to the users at the product or the manufacturer for free, in real-time, in a comprehensible format even including the necessary metadata to make use of the information. This will require major changes by manufacturers to make their products, services, and contracts compliant.

In the future, a logistics company, for example, will have access to all data that would normally be available to the manufacturers of their vehicles. It will allow the logistics company to extract data from their fleet to optimize its use, reduce consumption and conduct preemptive maintenance. The users can make the fleet information also available to third parties such as insurance, and leasing companies to create new data-driven business models.

On the other hand, **the manufacturers will only be able to make use of the data based on a contractual agreement with the users**, giving them control over their usage data.

Complementing the Data Governance Act, **the data will also be available to be shared in data spaces in a safe and regulated environment**.

A second important aspect of the Data Act is to facilitate switching between cloud and edge services. The obstacles to changing data processing services such as switching fees and unfair contract terms are to be removed. This is also a prerequisite for a data-driven economy.

Moreover, **the Data Act allows public authorities to access data held by companies in emergencies** for specific public interest purposes.

Finally, **the EU has built-in safeguards against unlawful data transfers by cloud service providers**. This should prevent third-country governments from gaining unlawful access to data.

In short, the key points are:

- **Right of users to obtain usage data generated by IoT devices.**
- **Limitations to use of data by manufacturers.**
- **Easier switching and exit for cloud and edge computing agreements.**

WHAT CAN YOU DO?

The Data Act gives consumers and businesses access and control over the data generated by their IoT products.

- **This will allow new business models for analysing and optimizing the use of products** e.g. using preemptive maintenance or allow better fleet management. Data will be available for sharing with third parties.
- **For manufacturers the new regulation means that products will need to designed to allow access to IoT data at the same quality as it is available to them.** Manufacturers also need to get contractual agreement to even use the IoT data for own purposes. Time is short as the new data sharing requirements will have to be implemented by 12 September 2025/2026.
- **Cloud service providers need to adapt their contracts and practices to facilitate switching and exit and abolish data egress fees.**

In brief, what do the regulations entail?

Artificial Intelligence Act

WHAT IS IT ABOUT?

The Artificial Intelligence Act (AI Act) provides the legal framework for the use of artificial intelligence in the EU. It aims to make the use of AI safer, more ethical and ensure the protection of individuals' rights.

The law divides AI systems into risk groups, amounting to three categories: prohibited, high risk and limited (low) risk.

Systems labelled as dangerous are banned by the AI act. Examples include biometric categorisation systems that classify natural persons based on sensitive or protected traits or characteristics, social scoring systems and systems that perform real-time biometric identification in public spaces.

AI systems that may have a significant risk of harm to health, safety or fundamental rights (or in some cases the environment) **are classified as "high risk" and are therefore subject to strict requirements**. Examples of high-risk AI systems include systems used for admission to educational institutions, for recruitment or selection of employees, assessing creditworthiness, assessing about access to government benefits and services and systems that influence voters of political campaigns.

If the AI is seen as "high risk", providers will have obligations on risk management, data management, quality management, transparency (including preparing documentation)**, logging, human oversight and conformity assessment.** In addition, a fundamental rights impact assessment must also take place. This should include the expected impact on fundamental rights, the foreseeable negative impact of the use of the system on the environment, as well as a detailed plan and explanation of how the negative impact on fundamental rights will be mitigated.

Additional transparency obligations have been included for lower-risk systems. These include systems used to interact with people (chatbots), biometric systems (including emotion recognition systems) to the extent they do not fall under prohibited systems.

Specific obligations are introduced for General Purpose AI, such as ChatGPT. **Basic models, also called foundation models, have a separate position within the AI act.** Both foundation models and high-risk systems should be registered in an EU database.

Finally, **it is worth noting that when developing and using AI systems, not only the AI Act applies. Intellectual property and privacy also play a role in the use of these systems**, and so regulations around them are also relevant.

Artificial Intelligence Act

WHAT CAN YOU DO?

If AI systems are used or developed within your company, the requirements from the AI Act should be adhered to and include attention to internal policies, terms and conditions and privacy documentation. In short:

- **If the application used falls within the definition of the AI act, transparency obligations come into effect.**
- **If the AI is considered "high risk", providers will have obligations on risk management, data management, quality management, transparency** (including preparing documentation), logging, human supervision and conformity assessment.
- **Users should use AI in accordance with the instruction manual**, assign human supervision to competent personnel and use relevant input data.
- **The GDPR plays an important role** both **when training AI** (the datasets used) **and when applying AI** (processing end-user data), compliance with the GDPR must be able to be demonstrated.

In brief, what do the regulations entail?

Digital Markets Act & Digital Services Act

WHAT IS IT ABOUT?

The Digital Services Act (DSA) and the Digital Markets Act (DMA) focus on online platforms. Both laws aim to create a safer digital space where users' fundamental rights are protected and a level playing field is created for businesses. The DMA focuses mainly on increasing online platforms' responsibility for the content posted on them. In particular, the DSA focuses on promoting a transparent and safe online environment for a range of digital service providers.

The DSA focuses on digital services, such as intermediary services providing network infrastructure (internet service providers, domain name registrars), **Hosting services** (cloud and web hosting services), **online platforms** such as online marketplaces, app stores, sharing economy platforms and social media platforms **and search engine**s, which act as mediators between users and content.

The DSA imposes obligations regarding transparency and handling of content (including content moderation and advertisements). This law consists of different regimes, depending on the organisation and services.

The most stringent regime applies to so-called "gatekeepers". Platforms with high user reach and impact are designated as "gatekeepers" and must provide additional information and monitor competition aspects.

These so-called gatekeepers are also covered by the DMA. **The DMA aims to regulate digital markets and address competition issues and includes rules on data, platform access, transparency, interoperability and more**. Only gatekeepers will have to comply with the DMA.

Thus, **the DSA applies not only to gatekeepers but also to smaller parties**, which are subject to a more lenient regime. However, if the creation of user-generated content for an online platform is only a secondary feature of the service, the DSA does not apply. In contrast, hosting services are subject to additional obligations.

The DMA targets only the largest parties, but also has the potential to have positive effects on smaller parties.

Digital Markets Act & Digital Services Act

WHAT CAN YOU DO?

The key actions under the DSA are:

- **Determining which category, and therefore which regime, you fall under.**
- **Updating your terms and conditions or terms of use**: providing information on procedures, measures and tools deployed for content moderation, algorithmic decision-making, and human control - in machine-readable format.
- **Set up notice and takedown mechanisms** (for filing and handling notifications about illegal content).
- **Setting up a complaint-handling system and providing information on it**, as well as dealing with illegal content (limiting visibility, suspending/terminating accounts, etc.).
- **Setting up a "know your customer" procedure**.
- **Track the average number of active users over the past 6 months** (also indicate on the website, unless micro or small business).
- **Nominate a contact point for government and report on website** (including an indication of languages in which can be communicated).
- **Nominate contact points for buyers** (natural persons) and report on website.
- If not located in the EU: specify legal representative in the EU.
- If aimed at minors: explain restrictions on the use of the service in a way that minors can understand.
- In case of suspicion of criminal offence committed or likely to be committed, threatening the life/safety of one/more persons: report to authorities.

For larger companies (from 50 employees, turnover from 12M or assets from 6M) **and very large platforms** (monthly 45M customers or more), **many additional obligations apply and specifically designated parties are also subject to the DMA**.

The DMA will have relatively little impact on **most companies**, but they **can benefit from its effects**:

- Business users who rely on gatekeepers to offer their services will have **more opportunities to counter abuse of dominance and** will have **new opportunities to compete and innovate in the online platform environment**, without having to comply with unfair conditions that limit their development.
- Developing alternative platforms/services will become more attractive as **consumers will have more opportunities to switch providers if they wish**.

In brief, what do the regulations entail?

Directive on Platform Work

WHAT IS IT ABOUT?

In the Directive on Platform Work, the European Union lays down rules on platform work. The directive applies to providers of well-known platforms, such as Uber, but also to employment agencies and (other) intermediaries. The directive applies not only to platform workers, but also to other self-employed workers.

The directive mainly improves two aspects.

First, **the directive helps determine the correct employment status of digital platform workers**. It harmonises the different regimes in the Member States regarding the qualification of a digital platform worker as self-employed or employed. This means that where an employment relationship does exist, even if it contradicts what was agreed between the parties on paper, this should also confer the employment and social rights associated with that employment relationship. What these rights entail depends on the national system.

Second, **it lays down rules for the use of artificial intelligence about the workplace**. Digital work platforms use algorithms to organise and manage platform work. The directive requires human monitoring of working conditions and provides for more transparency regarding the use of these algorithms, for example on how work is distributed. The directive also gives employees and self-employed workers the right to challenge automated decisions.

WHAT CAN YOU DO?

- **Assess whether your organisation meets the definition of a "digital work platform"**.
- **Be able to provide insight into how algorithms work** (which, incidentally, is also required under the GDPR).
- There are also a number of concerns from an employment law perspective. For more information, see: Consequences directive platform work self-employed contractor models - BDO.

In brief, what do the regulations entail?

Medical Device Directive

WHAT IS IT ABOUT?

The Medical Device Directive (MDR) has been amended so that certain medical software previously not covered by the directive and associated law can now be covered by the updated MDR and Medical Devices Act. The definition of a medical device has changed. Software is covered if it is intended by the manufacturer to be used alone or in combination with hardware for one or more specific medical purposes.

The directive consists of a tiered regime through risk classifications. Higher-risk classes naturally have stricter requirements, but the general safety requirements for medical devices are the same for all risk classes. The medical device risk classes have also been redesigned: software that was previously in the lowest risk class can therefore fall into a higher risk class.

WHAT CAN YOU DO?

- **Assess whether your software will be considered a medical device under the changed rules**, and if it already was, whether the risk classification changes.
- **If you sell software through an online platform, you must be able to provide an EU declaration of conformity** and comply with the requirements of Art 13, 14, 16 MDR.
- **For purchasers of software, it becomes important to check existing suppliers for having the correct CE marking and adjust procurement policies where necessary** (some software may no longer be approved under the new MDR).

In brief, what do the regulations entail?

DAC7

WHAT IS IT ABOUT?

The DAC7 directive was introduced in 2023 to bring further tax transparency to the digital economy.

The directive **creates a new annual reporting obligation for EU and non-EU operators of platforms that connect sellers with users for the sale of goods, rental of real estate, provision of personal services and rental of means of transport, through their digital platform** (website or application). For platform operators' reporting obligation, it does not matter whether a seller makes a profit or a loss. Nor does it matter whether the seller is an entrepreneur or an individual.

Platform operators are required to collect, verify and pass on information about the sellers using the relevant digital platform to the tax authorities. These include sellers based in the EU and parties renting property located in the EU.

WHAT CAN YOU DO?

- **BDO Netherlands has developed a tool to help determine whether a Platform Operator has reporting obligations under DAC7 or not** and the type of vendors to be reported, which is available at a fixed fee.
- **The first reporting deadline is 31 January 2024.** Failure to comply with reporting requirements can lead to administrative fines of up to €900,000 and prosecution.

In brief, what do the regulations entail?

NIS Directive 2

WHAT IS IT ABOUT?

In brief, the aim of the revamped Network and Information Security directive is to raise the level of cybersecurity among large and medium-sized organisations in "critical" sectors and increase cyber resilience. In addition, NIS 2 should also lead to improved cooperation between national governments of EU member states.

The new directive has a broader scope of application than its predecessor **and covers more sectors than its predecessor**. It also includes stricter security standards and incident reporting requirements.

The NIS2 is primarily relevant to large and medium-sized organisations operating in the sectors listed in Annexes I and II of NIS 2, which list a variety of critical sectors, such as energy, transport, banking, healthcare, drinking and wastewater and digital infrastructure. However it does not stop there: NIS2 also focuses on the entire supply chain. Even organisations that cannot themselves be characterised as essential but do business with these parties will be affected by the new directive. As a result, even small suppliers in SMEs may be affected by the obligations of the NIS2 directive.

WHAT CAN YOU DO?

You can already **assess whether your organisation operates in one of the sectors listed** in the NIS2 and will qualify as an "essential" or "important" organisation in terms of size, or does business with such a party and will be indirectly affected by it.

From the duty of care included in the NIS2, the necessary technical, operational and organisational measures will have to be implemented in your organisation, such as:

- **Risk analysis and information systems security policies**.
- **Directors should be trained to identify risks and assess risk management practices**.
- **Incident prevention and response** (basic measures around risk policy, incident handling risk policy, incident handling, backup management and contingency plans, cyber hygiene and training, encryption policy, multi-factor authentication, business continuity and crisis management).
- **Supply chain security**.
- **Security of network and information systems** (including proper response when vulnerabilities are disclosed).
- **Cybersecurity risk management policies and procedures.**
- **The use of cryptography and encryption.**
- **Cybersecurity information-sharing obligations.**
- **Setting up a "know your customer" procedure**.
- **Track the average number of active users over the past 6 months** (also indicate on the website, unless micro or small business).

In brief, what do the regulations entail?

Regulation Digital Operational Resilience for the Financial Sector (DORA)

WHAT IS IT ABOUT?

The Digital Operational Resilience Act (DORA), or digital operational resilience regulation for the financial sector, sets out requirements for the security of network and information systems of companies and organisations operating in the financial sector. These requirements also apply to external ICT service providers of these companies and organisations, such as providers of cloud services, software and data centres. Some external ICT service providers, such as micro-enterprises, fall outside the scope of DORA.

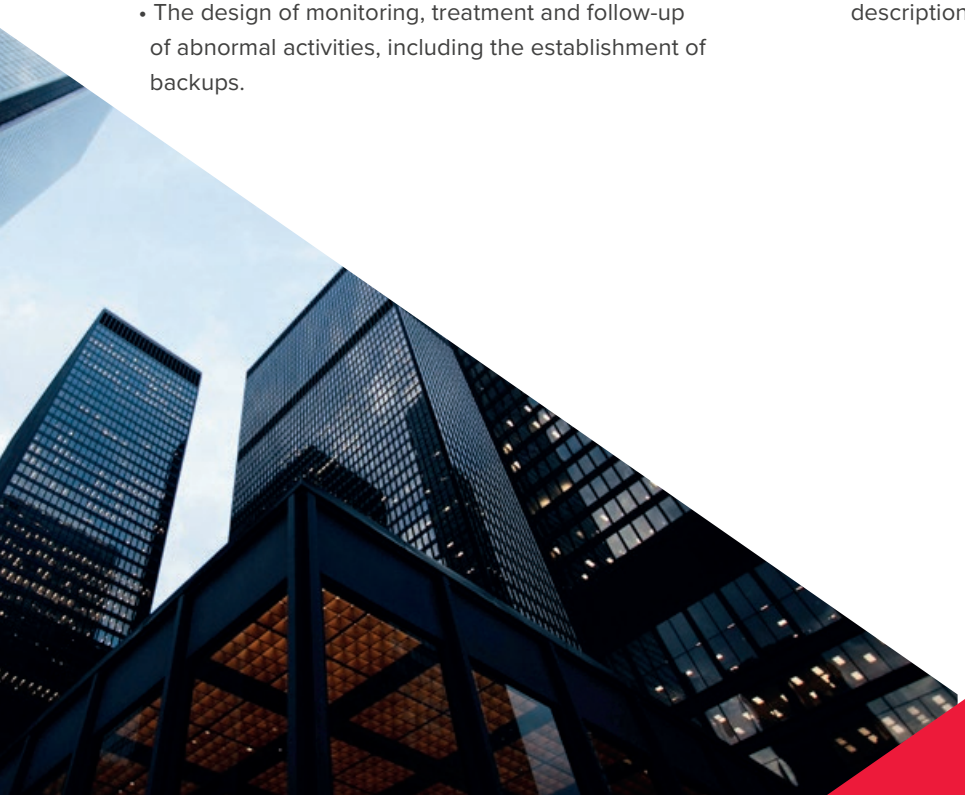
The new European Union regulation aims to ensure a uniform regime in IT compliance and aims to strengthen the IT security of financial entities, such as investment firms, insurance companies and banks.

DORA covers many different topics and requirements that can be roughly divided into five categories: 1) ICT risk management, 2) ICT-related incident management (classification and reporting), 3) periodic operational resilience testing, 4) risk management of and monitoring of third parties (ICT service providers) and 5) mutual sharing of cyber threat information.

WHAT CAN YOU DO?

DORA has been in force since 2023. However, companies have until January 2025 to comply. It is advisable to start analysing the current gap with DORA in good time and set up subsequent activities, such as:

- The ICT risk management framework, in line with the Enterprise Risk Management.
- The design of monitoring, treatment and follow-up of abnormal activities, including the establishment of backups.
- The ICT business continuity plan is tested periodically.
- Awareness programmes on IT, in line with the job description of employees.



Who can you contact?

Author

MICHA GROENEVELD
BDO Legal | Netherlands

micha.groeneveld@bdo.nl

ALBERT CASTELLANOS
BDO Legal | Spain

albert.castellanos@bdo.es

ANA TCHAIA
BDO Legal | Georgia

atchaia@bdo.ge

ASTRID EIKENES SKORPEN
BDO Legal | Norway

astrid.skorpen@bdo.no

GABRIELE FERRANTE
BDO Legal | Italy

gabriele.ferrante@bdo.it

ISTVÁN JÓKAY
BDO Legal | Hungary

istvan.jokay@bdolegal.hu

JIŘÍ ŠMATLÁK
BDO Legal | Czech Republic

jiri.smatlak@bdolegal.cz

KLAUS KROHMANN
BDO Legal | Switzerland

klaus.krohmann@bdo.ch

MAREK PRIESOL
BDO Legal | Slovakia

priesol@bdoslovakia.com

MATTHIAS NIEBUHR
BDO Legal | Germany

matthias.niebuhr@bdolegal.de

PIETER GOOVAERTS
BDO Legal | Belgium

pieter.goovaerts@bdo.be

RALUCA ANDREI
BDO Legal | Romania

raluca.andrei@tudor-andrei.ro

FOR MORE INFORMATION:

MENNO WEIJ
HEAD OF GLOBAL IP/IT
& PRIVACY WORKING GROUP
BDO LEGAL | NETHERLANDS

+31 6 109 190 24
menno.weij@bdo.nl

CAROLINE MACDONALD
COORDINATOR | LEGAL SERVICES
BDO GLOBAL OFFICE

+34 686 339 922
caroline.macdonald@bdo.global